INFORMATION RESOURCE CENTER
AMERICAN EMBASSY
BUDAPEST, HUNGARY

Information Technology E-Government and E-Commerce

July 2005

N E W S L E T T E R N O . 2 0

INFORMATION AND COMMUNICATION

Government Documents

FTC Cracks down on Illegal "X-rated" Spam
E-Mail Exposed Children, Others, to Graphic Content
For Release: July 20, 2005

In a crackdown on operations that illegally expose unwitting consumers to graphic sexual content, the Federal Trade Commission has charged seven companies with violating federal laws requiring warning labels on e-mail that contains sexually-explicit content. U.S. District Court suits filed against three operations seek civil penalties and a permanent bar on the illegal marketing. Settlements with four other operations have imposed $1.159 million in civil penalties. The settlements bar the illegal marketing practices in the future and require that the defendants monitor their affiliates to ensure they are not violating the law.

http://www.ftc.gov/opa/2005/07/alrsweep.htm

Federal Communications Commission Releases Data On High-Speed Services For Internet Access
July 7, 2005
High-Speed Connections to the Internet Increased 34% During 2004 for a Total of 38 Million Lines in Service

Washington, D.C. - The Federal Communications Commission (FCC) today released new data on high-speed connections to the Internet in the United States. Twice a year, facilities-based broadband providers must report the number of high-speed connections in service pursuant to the FCC's local competition and broadband data gathering program (FCC Form 477).
For reporting purposes, high-speed lines are connections that deliver services at speeds exceeding 200 kilobits per second (kbps) in at least one direction, while advanced services lines are connections that deliver services

at speeds exceeding 200 kbps in both directions.
For the purposes of this report we collected data from providers with at least 250 high-speed lines in a state. Statistics released today reflect data as of December 31, 2004 filed by providers on FCC Form 477 in the Commission's local competition and broadband data gathering program.

http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOK-259870A1.doc
Full text of report:
http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/hspd0705.pdf

Ten Nations Join U.S. in Internet Piracy Crackdown (2005-07-01)

The U.S. Federal Bureau of Investigation and law enforcement authorities from 10 other nations conducted more than 90 searches starting June 29, intending to dismantle criminal groups engaged in illegal acquisition, sale and distribution of copyrighted software, movies, music and games.
U.S. Attorney General Alberto Gonzales announced June 30 an effort the department has labeled “Operation Site Down.” A Justice Department press release describes the operation as an attempt to disrupt the top tier in the copyright piracy supply chain.
“And by penetrating this illegal world of high technology and intellectual property theft,” Gonzales said, ”we have shown that law enforcement can and will find – and we will prosecute – those who try to use the Internet to create piracy networks beyond the reach of law enforcement.”
The operation is working to undermine what’s known as the “warez scene,” the illegal online trade in software and entertainment products. Warez, pronounced "wares," is from the plural of the word software.
The investigations focus on organizations and individuals who are thought to be "first-providers" of copyrighted works to warez networks.
A warez group can release a stolen film or recording, for instance, to servers throughout the world within minutes. After that, unsanctioned copies of the works filter through the Internet on various peer-to-peer networks.
The other nations involved in the sweep are Canada, Israel, France, Belgium, Denmark, the Netherlands, United Kingdom, Germany, Portugal and Australia.

http://www.uspolicy.be/Article.asp?ID=4416C76F-F4E8-4BCC-A64E-7FD0E3BA0102

U.S. Intends To Preserve Security of Internet Domain System (2005-07-01)

The U.S. National Telecommunications and Information Administration (NTIA) issued a new statement of policy June 30, expressing the U.S. intent to maintain its oversight of the operation of the Internet’s Domain Name and Addressing System (DNS).
DNS is the system that allows online users to name Web pages and e-mail boxes and allows Internet applications to read and recognize those names so users can reliably navigate online.
This system relies on 13 root servers that are privately operated computers containing the files that list names and numeric Internet protocol addresses of the DNS servers for all top-level domains (TLDs) such as dot-org, dot-com, dot-edu, dot-int and others. Established by the U.S. Commerce Department in 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) decides what goes in those files.
The NTIA statement calls for ICANN to maintain its position as the appropriate technical manager of the

Internet DNS.
In the international discussion of Internet management, some governments and groups advocate different forms of Internet governance, a matter that will receive further attention with the approach of the World Summit on the Information Society to be held in Tunis in November. As a prelude to that meeting, a U.N. panel is preparing new recommendations on Internet management.
The U.S. policy statement also acknowledges the interests governments have in managing their country code top-level domains, and expresses commitment to working with governments to address sovereignty concerns while ensuring DNS stability.
A detailed explanation of DNS is available on the Web site of the Internet Society at http://www.isoc.org/briefings/019/; a professional membership society with more than 100 organization and over 20,000 individual members in over 180 countries.

http://www.uspolicy.be/Article.asp?ID=8D9449A8-CECC-485E-97B0-15FDDB4B16AE

05AD557 HEALTH INFORMATION TECHNOLOGY: HHS IS TAKING STEPS TO DEVELOP A NATIONAL STRATEGY. [GAO-05-628]

United States Government Accountability Office (GAO). May 27, 2005; Web-posted May 31, 2005.

Health Information Technology (IT) is used to support health care quality and efficiency by providing tools to improve patient care and to reduce administration overhead. Examples include the following:
* Electronic health records (EHRs) provide patients and their caregivers the necessary information required for optimal care while reducing costs and administrative overhead, such as that associated with patient registration, admission, discharge, and billing.
* Computer-assisted clinical decision support tools increase the ability of health care providers to take advantage of current medical knowledge from online medical references as they make treatment decisions.
* Computerized provider order entry allows providers to electronically order tests, medicine, and procedures for patients, reducing errors associated with hand-written orders and prescriptions.
* Telehealth is used to provide health care to rural and remote areas through the use of communications technologies.
To prevent medical errors, reduce costs, improve quality, and produce greater value for health care expenditures, President Bush has called for the Department of Health and Human Services (HHS) to develop and implement a strategic plan to guide the nationwide implementation of health information technology in both the public and private health care sectors. The Departments of Defense (DOD) and Veterans Affairs (VA), along with other countries, have already taken steps to improve health care delivery and administration by implementing IT solutions. GAO was asked to provide an overview of HHS's recent efforts to develop a national health IT and to identify lessons learned from DOD's, VA's, and other countries' experiences in implementing health IT.
From DOD and VA, GAO provides the following lessons:
* Obtain full endorsement of top leadership,
* define and adopt common standards and terminology,
* recognize and address the needs of the varied stakeholder communities, and
* deploy in small increments and build on success.
Among lessons learned from initiatives in Canada, Denmark, and New Zealand to establish national health IT infrastructures with government support and identified lessons learned from their experiences are these:
* Focus on creating standards first,
* establish a central organization to lead health IT efforts, and

* implement solutions incrementally.

http://www.gao.gov/new.items/d05628.pdf [pdf format, 92 pages]

New Super Computer Targets Physics Research (2005-05-27)

A new computer was unveiled May 26 at a dedication ceremony at the U.S. Department of Energy (DOE) Brookhaven National Laboratory (BNL) in New York. Physicists from around the world attended the event. According to a DOE press release, the supercomputer was designed and built by BNL, Columbia University, IBM, the Institute of Physical and Chemical Research (RIKEN) in Japan and the University of Edinburgh. The $5 million supercomputer took three years to build and is funded by RIKEN, with infrastructure support from DOE's Office of Science.

The supercomputer, housed at the RIKEN BNL Research Center, is called QCDOC, for quantum chromodynamics on a chip. Quantum chromodynamics is a theory in physics that describes the interactions of subatomic particles called quarks and gluons.

The computer has 10 teraFLOPS of peak computing power, which makes it capable of performing 10 trillion arithmetic calculations per second, with sustained speeds of five teraFLOPS. QCDOC achieves its ultrafast speed by harnessing the power of 12,288 individual computers, each with its own memory, and an extremely fast interprocessor communication network.

FLOPS is an acronym for floating-point operations per second, a common measurement for rating the speed of microprocessors. Floating-point operations include any operations that involve fractional numbers. A teraFLOPS, or TFLOPS, is equal to one trillion floating-point operations per second.

QCDOC will be used for physics research for 90 percent of its operating time. During the remaining operating time, researchers will use the supercomputer to pursue scientific projects in a variety of fields, including biology and materials science.

The RIKEN-BNL QCDOC is one of three similar computers that have been built by the same team of collaborators.

Working on related and sometimes different problems using these three supercomputers, researchers hope to make significant contributions in physics and other scientific fields.

http://www.uspolicy.be/Article.asp?ID=A24E558F-C468-41C8-BB6E-BAEC6CA748A0

05AD538 INFORMATION SECURITY: FEDERAL AGENCIES NEED TO IMPROVE CONTROLS OVER WIRELESS NETWORKS. [GAO-05-383]
United States Government Accountability Office (GAO). May 17, 2005.

The use of wireless networks is becoming increasingly popular. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops. They can offer federal agencies many potential benefits but they are difficult to secure. GAO was asked to study the security of wireless networks operating within federal facilities. This report (1) describes the benefits and challenges associated with securing wireless networks, (2) identifies the controls available to assist federal agencies in securing wireless networks, (3) analyzes the wireless security controls reported by each of the 24 agencies under the Chief Financial Officers (CFO) Act of 1990, and (4) assesses the security of wireless networks at the headquarters of six federal agencies in Washington, D.C.

GAO found that federal agencies have not fully implemented key controls such as policies, practices, and tools

that would enable them to operate wireless networks securely. Further, GAO tests of the security of wireless networks at six federal agencies revealed unauthorized wireless activity and "signal leakage" -- wireless signals broadcasting beyond the perimeter of the building and thereby increasing the networks' susceptibility to attack. [Note: For security reasons, GAO does not identify those agencies in this report.] Without implementing key controls, agencies cannot adequately secure federal wireless networks and, as a result, their information may be at increased risk of unauthorized disclosure, modification, or destruction.

http://www.gao.gov/new.items/d05383.pdf [pdf format, 31 pages]

05AD522 VIDEO NEWS RELEASES: UNATTRIBUTED PREPACKAGED NEWS STORIES VIOLATE PUBLICITY OR PROPAGANDA PROHIBITION.
TESTIMONY OF SUSAN A. POLING BEFORE THE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, U.S. SENATE. [GAO-05-643T]
United States Government Accountability Office (GAO). May 12, 2005.

In recent years, federal agencies have been increasing their use of video news releases (VNRs), which frequently include prepackaged news stories. While the use of VNRs is widespread and widely known by those in the media industry, the quality and content of materials considered to constitute a VNR can vary greatly. Generally, a VNR package may contain several items, including a series of video clips, known as B-roll footage; title cards containing relevant information, known as slates; a prepackaged news story, referred to as a story package; and other promotional materials. These materials are produced in the same manner as television news organizations produce materials for their own news segments. The prepackaged news stories are distributed to local television news stations and are designed to resemble actual news stories. By eliminating the costs and effort of producing an original news story, agencies can find news stations willing to broadcast a favorable news segment on a desired topic. GAO examined prepackaged news stories produced by the Department of Health and Human Services and the Office of National Drug Control Policy and evaluated whether these materials constituted covert propaganda in violation of the prohibition on using appropriated funds for publicity and propaganda not authorized by Congress.
This following states the position of the General Counsel of GAO: "While agencies generally have the right to disseminate information about their policies and activities, agencies may not use appropriated funds to produce or distribute prepackaged news stories intended to be viewed by television audiences that conceal or do not clearly identify for the television viewing audience that the agency was the source of those materials. It is not enough that the contents of an agency's communication may be unobjectionable. Neither is it enough for an agency to identify itself to the broadcasting organization as the source of the prepackaged news story.

http://www.gao.gov/new.items/d05643t.pdf [pdf format, 12 pages]

WORLD RADIOCOMMUNICATION CONFERENCES
Recommendations for Improvement in the United States Preparatory Process
Pinciple Author: Darlene A. Drazenovich. Special report
U.S. DEPARTMENT OF COMMERCE, National Telecommunications and Information Administration. NTIA Report 05-427 May 2005

The United States' radiocommunication interests are global. Communications are the backbone of our eco-

nomic and national security and radiocommunications are a critical component of the United States' overall communications interests. Radio signals traverse borders, oceans and space. The mobility of radio systems leads to services, technologies, and operations that span the global community and economy. The successful development and implementation of radiocommunications depend on international agreements reached at World Radiocommunication Conferences (WRCs). These conferences meet every three to four years under the auspices of the International Telecommunication Union (ITU) to update the international radio regulations on the use of the radio spectrum. The ITU is a specialized agency of the United Nations, and has 189 member states. The outcome of WRCs provides the international regulatory framework for the use of radiocommunication systems vital to U.S. economic growth, U.S. national security, safety of life and property, and scientific investigations. The United States must continue its success at these international conferences in negotiating spectrum allocations and regulations forward-looking and flexible enough to accommodate technologies and operations that the United States will need in the future.

http://www.ntia.doc.gov/reports/wrc/wrc_05232005.htm
http://www.ntia.doc.gov/reports/wrc/wrc_05232005.pdf

Radio Frequency Identification: Opportunities and Challenges in Implementation, Department of Commerce, April 2005

The Department of Commerce has released an information paper on "Radio Frequency Identification: Opportunities and Challenges in Implementation." NTIA participated on the RFID Working Group that developed this paper.

As is common with emerging technologies, several challenges must be overcome for the technology to mature to its full potential. In the case of RFID, these challenges include: maturation of RFID technology, harmonization of standards for hardware/software and wireless spectrum operations, privacy and security concerns, and implementation cost barriers. As these technical and policy challenges are mitigated, RFID will likely become the system of choice for global commerce.

Interoperability across various RFID systems, companies, and countries is critical to achieving wide-scale deployment of RFID technology. Development of technical standards for tags, readers, and interface systems; and allocation of operational limits for frequency and transmission power will determine global interoperability.

Initial system and implementation costs are still being refined; in the near-term this could prove to be an impediment to large-scale adoption. Within small and medium-sized enterprises, although RFID provides them with new opportunities to compete in the global market, limited budgets, lack of in-house expertise, and a lack of access to new technologies could be an impediment for adoption.

The collection and use of personally identifiable information through RFID technologies represents a key public policy challenge to the deployment and use of RFID technologies.

Much of this concern is with the collection, use, and storage of the data rather than the technology itself. Industry-driven solutions are beginning to include a combination of operational guidelines, technical solutions, and educational campaigns.

Summary: **http://www.technology.gov/Events/2005/RFID/0406_1-page.pdf**
Full report: **http://www.technology.gov/reports/2005/RFID_April.pdf**
http://www.technology.gov/reports/2005/RFID_April.doc

Think Tank Publications

Public Awareness of Internet Terms
Lee Rainie. 7/20/2005
PEW Internet & American Life Project

Large numbers of internet users do not know the basic definition of some of the hottest new internet innovations and one of the most serious online dangers.
In a nationwide phone survey between May 4 and June 7, the Pew Internet & American Life Project asked internet users if they knew what certain internet terms meant. The results showed that some terms were well known, but that the terms "podcasting" and "RSS feeds" were not familiar to a majority of internet users and that "phishing" is still a foreign term to many.

http://www.pewinternet.org/pdfs/PIP_Data_Techterm_aware.pdf

Report of the Working Group on Internet Governance
WGIG. June 2005.

An independent working group has released a report on Internet governance proposing to improve Internet governance arrangements and setting priorities for future action. The report from the Working Group on Internet Governance (WGIG) will be considered during the second phase of the World Summit on the Information Society (WSIS) in November in Tunis, Tunisia. According to a July 15 U.N. press release, governments could not agree on questions about Internet control and management at the first phase of WSIS in 2003 in Geneva and asked the U.N. secretary-general to establish a working group to help make decisions in the summit's second phase. The WGIG report also proposed further internationalization of Internet governance arrangements, based on a 2003 WSIS declaration of principles that advocates multilateralism and the involvement of international organizations and all parties with a vested interest. The report identified a wide range of governance functions but recommended excluding government involvement in day-to-day operational management of the Internet. It also proposed creation of a global forum to discuss problems linked to Internet governance, including spam and cybercrime.

http://www.uspolicy.be/Article.asp?ID=8963F9BF-8936-434C-B5A5-08DFF235EC47
The report is available on the WGIG and WSIS websites:
http://www.wgig.org/
http://www.itu.int/wsis/.

05AD570 SPYWARE: THE THREAT OF UNWANTED SOFTWARE PROGRAMS IS CHANGING THE WAY PEOPLE USE THE INTERNET.
Susannah Fox. Pew Internet & American Life Project. July 2005.

The Pew Internet & American Life Project set out to measure the impact of the recent wave of online activity related to spyware and adware. Spyware is software that is placed secretly on a computer in order to track a user's behavior and report back to a central source. Adware, on the other hand, is software that comes bundled as a package with programs that consumers download, and is used to serve up targeted advertising based on the user's online behavior.

The researchers wanted to know: Do average Internet users understand the basic concepts? How many are dealing with the problems commonly associated with unwanted software programs? And are they taking steps to prevent software intrusions? Survey questions were developed in consultation with consumer advocates, adware company executives, and security experts. Interviews with 1,336 Internet users were conducted May 4 - June 7, 2005.
The researchers found that the threat of unwanted software programs is making people more cautious online. Most Internet users think symptoms of spyware are serious problems rather than simply minor annoyances. Millions of Internet users have first-hand experience with computer problems related to software intrusions and while many express confidence and knowledge of the issues, most think more should be done to guard against spyware and to notify people about adware.
[Note: Contains copyrighted material.]

http://www.pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf [pdf format, 23 pages]

Privacy in the Workplace
Case Studies on the Use of Radio Frequency Identification in Access Cards
RAND. RB-9107-RC (2005)

Companies use RFID workplace access cards to do more than just open doors (e.g., for enforcing rules governing workplace conduct). Explicit, written policies about how such cards are used generally do not exist, and employees are not told about whatever policies are being followed. Using such systems has modified the traditional balance of personal convenience, workplace safety and security, and individual privacy, leading to the loss of "practical obscurity." Such systems also raise challenges for the meaning and implementation of fair information practices.

http://www.rand.org/publications/RB/RB9107/

E-GOVERNMENT AND E-COMMERCE

Congressional Documents (Hearings, Reports, etc.)

05AD523 INFORMATION MANAGEMENT: IMPLEMENTATION OF THE FREEDOM OF INFORMATION ACT. TESTIMONY OF LINDA D. KOONTZ BEFORE THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE AND ACCOUNTABILITY, COMMITTEE ON GOVERNMENT REFORM, HOUSE OF REPRESENTATIVES. [GAO-05-648T]
United States Government Accountability Office (GAO). May 11, 2005

The Freedom of Information Act (FOIA) establishes that federal agencies must provide the public with access to government information, thus enabling them to learn about government operations and decisions. To help ensure appropriate implementation, the act requires that agencies report annually to the Attorney General, pro-

viding specific information about their FOIA operations. GAO was asked to describe the FOIA process and discuss the reported implementation of FOIA.
Although the specific details of processes for handling FOIA requests vary among agencies, the major steps in handling a request are similar across the government. Agencies receive requests, usually in writing (although they may accept requests by telephone or electronically), which can be submitted by any organization or member of the public. Once requests are received, the agency responds through a process that includes several phases: initial processing, searching for and retrieving responsive records, preparing responsive records for release, approving the release of the records, and releasing the records to the requester. According to data reported by agencies in their annual FOIA reports, citizens have been requesting and receiving an ever-increasing amount of information from the federal government through FOIA. The number of requests that agencies received increased by 71 percent from 2002 to 2004. Further, agencies reported they have been processing more requests--68 percent more from 2002 to 2004. For 92 percent of requests processed in 2004, agencies reported that responsive records were provided in full to requesters. However, the number of pending requests carried over from year to year--known as the backlog--has also been increasing, rising 14 percent since 2002.

http://www.gao.gov/new.items/d05648t.pdf [pdf format, 29 pages]

Think Tank Publications

Electronic Prescribing Systems
Making It Safer to Take Your Medicine?
RAND. RB-9052-RC (2005)

Electronic prescribing systems may greatly reduce medication errors, thereby maximizing patient safety and health.
Menus that aid in selecting appropriate medication doses and other specific features are important for achieving these goals.
Currently used electronic prescribing systems vary widely in their features and capabilities and may not produce the best results for patient safety and health, but it should be possible to implement about two-thirds of the guidelines in the next three years.

http://www.rand.org/publications/RB/RB9052/

A National Study of E-Recruitment in State Governments
Soonhee Kim (Syracuse University); Jennifer Greenwood O'Connor (Syracuse University)
Campbell Public Affairs Institute, The Maxwell School of Syracuse University
Working Paper No. 4 April 2005

Government service delivery is undergoing rapid change because of innovations in Information Technology (IT) tools (e.g., the Internet and Geographic Information Systems [GIS]) that are being used by governments at all levels to improve external collaboration, civic engagement, networking, and customer service. IT expansion is also creating new challenges for human resource management in the public sector. There is growing evidence that organizations in the private and public sector are using Internet technology and the World Wide

Web as a platform for recruiting and testing candidates (Cober, Brown, Blumental, Doverspike, and Levy, 2000). Online recruitment or electronic recruitment (e-recruitment), embracing the term web-based recruiting, can be described as any recruiting processes that an organization conducts via web-based tools, such as the organization's public Internet site or its corporate intranet (Kerrin and Kettley, 2003). The term online recruitment, or e-recruitment, also implies the formal sourcing of job information online.

http://www.maxwell.syr.edu/campbell/Library%20Papers/04-05%20Working%20Papers/Kim04-05.pdf

Szilágyi Ágota 475-4442
Keve Ildikó 475-4478
Bíró Katalin 475-4514
Staff of the Information Resource Center

e-mail: infousa@usembassy.hu
FAX: 475-47-08